International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 3, Issue 5, Dec 2013, 1-8
© TJPRC Pvt. Ltd.

PERFORMANCE ANALYSIS OF SPREAD SPECTRUM ALGORITHM INTACTING THE INFORMATION IN AUDIO SIGNALS

HEENA MALIK[1] & SANDEEP SINGH KANG[2]

[1]Assistant Professor, Computer Science & Engineering, Chandigarh University, Chandigarh, India

[2]Head of Department, Computer Science & Engineering, Chandigarh Group of College, Landran, Mohali, Punjab, India

ABSTRACT

Audio steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. The major challenge in audio steganography is that to obtain robust high capacity steganographic systems. This paper presents a secure data transfer technique using Cryptography and Audio Steganography for mobile network. The combination of SS technique with XORing method is described in this paper, which provides good level of security.Number of techniques for embedding information in digital audio has been established. We will attend the general principles of hiding secret information using audio technology. Spread spectrum (SS) technique has developed rapidly in this area due to the advantages of good robustness and immunity to noise attack. The spread-spectrumtechniques for watermarking are very popularnowadays. Two types of spread spectrum techniques areused direct sequence spread spectrum (DSSS) and frequencyhopped spread spectrum (FHSS). Implementation of steganography in audio data using Direct Sequence Spread Spectrum method has been presented in this thesis. A key is needed to embed messages into noise. This key is then used to generate a key sequence. The information you want embed must first modulated using that key sequence. Also, Random location selection to embed the data within the cover audio is also proposed in the work. These modifications give a more secure stegano-graphic system,making guesses about the bit-rate or message length less feasible. The proposed stegano and extraction system uses DSSS technique. These are used to increase the security as well as robustness. Improvement has been attained in robustness on the expense of reducing the capacity of hiding. The imperceptibility of the stego audio and extracted image is assessed by using peak signal-to-noise ratio (PSNR) and normalized correlation measure.

KEYWORDS: Audio Steganography, Cryptography, Least Spread Spectrum (SS) Technique, Information Security, Secret Key

INTRODUCTION

Watermarking has been a copyright protection technology for a while. Spread Spectrum (SS) watermarking technique is used in this era for audio copyright protection. Compared with existing technologies, the robust character of SS is the reason of selecting it.[1] Other than copyright watermarking, audio SS technology is also very suitable for providing robust cover channel. But, unfortunately, implementation is less based as audio cover channel. The internet security problems provide the opportunity for this technology since online audio sharing is very popular now a days.[3] Users can use the audio cover channel to send security information without being detected and attacked by hackers easily,Spread spectrum technology has developed rapidly in the area of hiding secret information. In audio steganography, spread spectrum has accepted extensive attention owing to the advantages of good immunity to steganalysis. Usually, the steganalysis algorithms for audio cover may achieve some satisfactory detection results.[5] This method of hiding directly appropriate for audio cover, due to different characteristics of audio signals. The statistical regularities captured in audio signals are inherent to the spatial composition of images that are simply not present in audio.[8] As to audio steganalysis field, all these algorithms attempt to find good feature vectors from time domain or transform domain which are used to capture statistical changes caused by data embedding. But these features are not effective to spread-spectrum steganographic embedding.

In this paper, we aim to propose two effective algorithms of extracting feasible feature vectors for SS hiding as to get higher detecting accuracy, compared with the present steganalysis algorithms for DSSS hiding. The proposed algorithm is based on PSNR theory. The paper is organized as follows. Section 2 we introduce the related work of this field. Sections 3 and Section 4 we describe our proposed algorithms and give results.

RELATED WORK

A lot of work has been done in the field of information hiding in the context of the spread spectrum technology. Due to space limitations, we only provide an overview of related approaches. Most of the work published is put under the focus of digital watermarking [7]. In contrast, our approach relates with another aspect of information hiding, namely steganography. The main difference between these two techniques is the fact, that watermarks are public and their Usage is known by everybody. In the field of steganography, the existence of hidden information is only known by the communication partners [14]. The prevention of various types of attacks has also to be dealt .While our focus lies on auditive data as cover media, which could be Voice over WAV-files or samples recorded from a sound card, many publications in the field of watermarking only link with digital images. Our work distinguishes itself from other published work in the audio steganography field in important aspects. Issues like the synchronisation of sender and receiver are improved by our solution. .

Steganography History

The first use of information hiding was back to the ancient Greeks. Herodotus tells how a message was passed to Greeks underneath the wax of a writing tablet, and describes a technique of dotting successive letters in a cover text with secret ink.[15] In ancient China, people were using a technology: embedding a code at a prearranged position in a dispatch. During World War second the method or some variants were used by spies.[12] In the same period, the Germans developed microdot technology to print a good quality photograph shrunk to the size of a dot. In the current industry market, with the advent of digital communication and, one important issue is copyright enforcement, which is commonly implemented.

SPREAD SPECTRUM INTRODUCTION

Spread Spectrum techniques are widely used in data communication, such as the CDMA mobile communication. The first patent work was published by Hedy Lamar and George Antheil in 1941 for providing secret communication for military purposes.[8] Spread Spectrum techniques are methods of energy generated in particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. Some of technologies exist in this branch.

- DSSS stands for Direct Sequence Spread Spectrum. Data to be transmitted is divided into small pieces and each piece is allocated to a frequency channel across the spectrum. Transmitter utilizes a phase varying modulation technique to modulate each piece of data with a higher data rate bit sequence. [10]
- FHSS stands for Frequency-Hopping Spread Spectrum. It is a method of transmitting signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both the transmitter and receiver.[10]

- THSS stands for time-hopping Spread Spectrum. Short information bursts [chirps] are transmitted with pseudorandom pulse durations, or transmitted in random positions. Generally, there are two methods to implement this.

Method 1

The chirp interval is determined by the PN code generator.

Method 2

The chirp goes at the same time in each bit period, the PN generator changes its duration. Here, a chirp is a signal in which the frequency increases or decrease with time. General Spread Spectrum application by using chirps is also called Chirp Spread Spectrum [CSS] Quite often, the researcher combines these technologies together to produce some new patterned Spread Spectrum technology.

THE SPREAD SPECTRUM TECHNIQUE

Before entering the description of our proposed system, this section recalls some important aspects of the spreading and de-spreading processes.

In a DSSS system, a signal of low bandwidth is spread over a broad frequency range. Hence the power of the signal is decreased and thus the signal vanishes in the noise of the cover media.[13] To extract an embedded signal from the cover, the receiver needs knowledge about the spreading process. This knowledge can therefore be described as a kind of secret key, needed as input to the system. At the sender, each bit is first converted to a sequence of chips, thus increasing the bandwidth while decreasing the signal power. Pseudo-noise (PN) chip sequences are generated using a linear feedback shift register (LFSR). The length of an output sequence depends on the number of stages. In general, m-sequences are preferred, depicting the maximum length of a generated sequence without repetitions.

EMBEDDING AND EXTRACTION ALGORITHM

The spread spectrum method attempts to spread secret information across the audio signal. This is analogous to a system using an implementation of the LSB coding which randomly spreads the message over the entire sound file. However, unlike LSB coding, the Spread Spectrum Technique spreads the secret message over the audio file's frequency spectrum, using a code that is independent of the actual audio signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. The proposed algorithm is given below:

EMBEDDING ALGORITHM

Inputting and reading of watermark image and cover audio signal.

- Generation of random key sequence so as to decompose watermark.
- Division of cover audio into two parts so as to hide watermark information into 1st part.
- Establishment of empty cell array, so as to put elements blockwise (size=10) of 1st part of cover audio.
- Conversion of 1st part audio into array of column matrix (each matrix have 10 elements).
- Modification of a specific element of each sub matrix in accordance with each watermark element.
- Conversion of array into a single matrix and addition with 2nd part of cover audio.

EXTRACTION ALGORITHM

- Division of both audio i.e. marked and original into two parts i.e. 1st and 2nd.
- Declaration of empty cell having array of empty matrices so as to fill these with first part of both matrices.
- Application of discrete cosine transform on both cells.
- Division of 3rd element of each matrix of watermarked audio signal by that of original audio cover signal.
- Decoding of watermark components or removal of key sequence.
- Reconstruction of extracted watermark according to size of original watermark image.

PERFORMANCE METRIC

After simulation of program some results or output parameters i.e. value of PSNR, computational time and value of normalized correlation has been driven along with some figures, representing input and output from the simulation. First two figures are derived from simulation for embedding of watermark image in cover audio signal Figure 1 has been divided into two parts 1st part shows the plot of frequency coefficients of cover audio signal and 2nd part shows the plot of frequency coefficients of watermarked audio signal, so as to compare cover and watermarked audio signal. It can be easily seen that both have almost characteristic and almost similar, which can be proved by Normalized correlation value i.e. 0.9995. Figure 2 is the snapshot of command window, shows the value of other two mentioned parameters. The PSNR value of embedded audio signal is 103.8254 dB. The time which elapsed during whole simulation is 2.2308s. Next two figures have been driven from the extraction simulation of watermark. Figure 3 is also divided into two parts, so as to compare original watermark image and extracted watermark image. The similarity between both images can be described by Normalized correlation value i.e. 0.8642. Figure 4 is the snapshot of command window, shows the value of other two mentioned parameters. The PSNR value of extracted watermark is 64.4317dB. The time which elapsed during whole simulation is 1.6692s. If we compare both the watermark analytically both have no difference, which is a good sign for proposed method in terms of correlation.

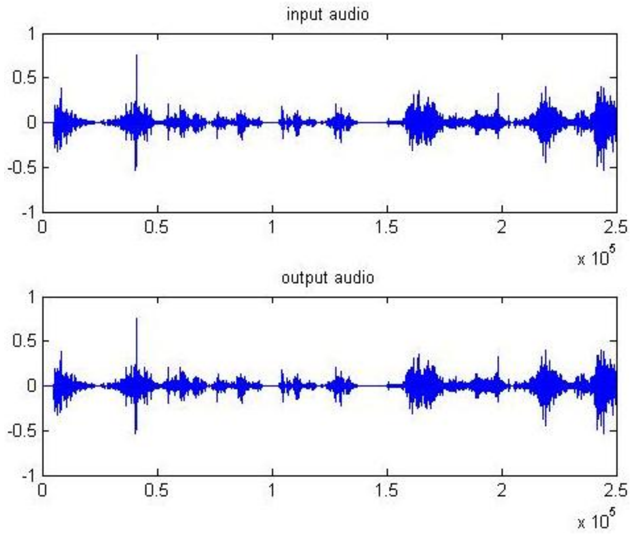
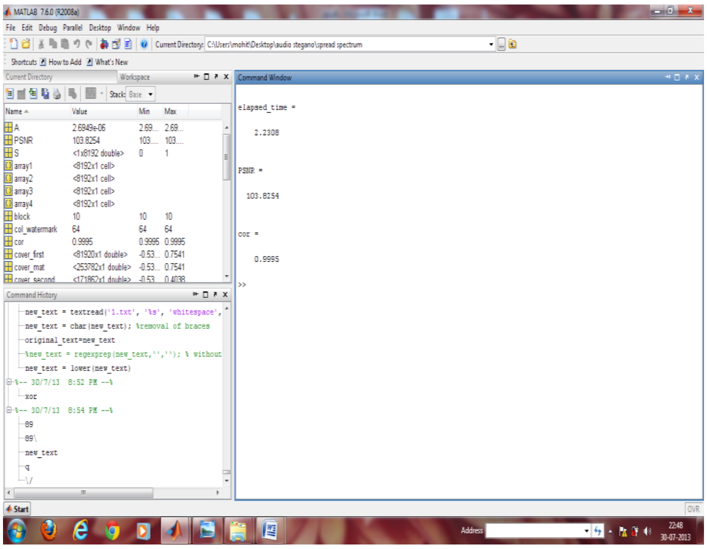


Figure 1: Comparison Original Cover Audio Signal and Embedded Audio Signal


MATLAB 7.6.0 (R2008a)
File Edit Debug Parallel Desktop Window Help
Current Directory: C:\Users\mohit\Desktop\audio stegano\spread spectrum
Shortcuts How to Add What's New
Current Directory
Workspace
Stack: Base
Command History
Command Window
Start
Address
22:48
30-07-2013

```
Name        Value             Min     Max
A           2.6949e-06        2.69... 2.69...
PSNR        103.8254          103.... 103....
S           <1x8192 double>   0       1
array1      <8192x1 cell>
array2      <8192x1 cell>
array3      <8192x1 cell>
array4      <8192x1 cell>
block       10                10      10
col_watermark 64              64      64
cor         0.9995            0.9995  0.9995
cover_first <81920x1 double>  -0.53... 0.7541
cover_mat   <253782x1 double> -0.53... 0.7541
cover_second <171862x1 double> -0.53... 0.4038
```

```
new_text = textread('1.txt', '%s', 'whitespace',
new_text = char(new_text); %removal of braces
original_text=new_text
%new_text = regexprep(new_text,'',''); % without
new_text = lower(new_text)
%-- 30/7/13  8:52 PM --%
xor
%-- 30/7/13  8:54 PM --%
89
89\
new_text
q
\/
```

```
elapsed_time =

    2.2308


PSNR =

  103.8254


cor =

    0.9995

>>
```

Figure 2: Snapshot of Command Window for Embedding of Watermark

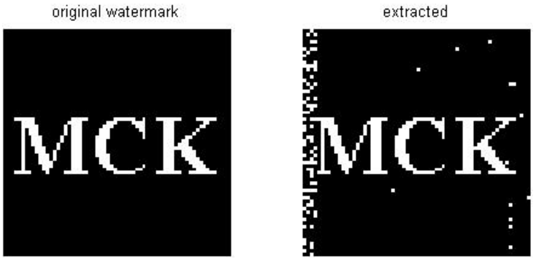
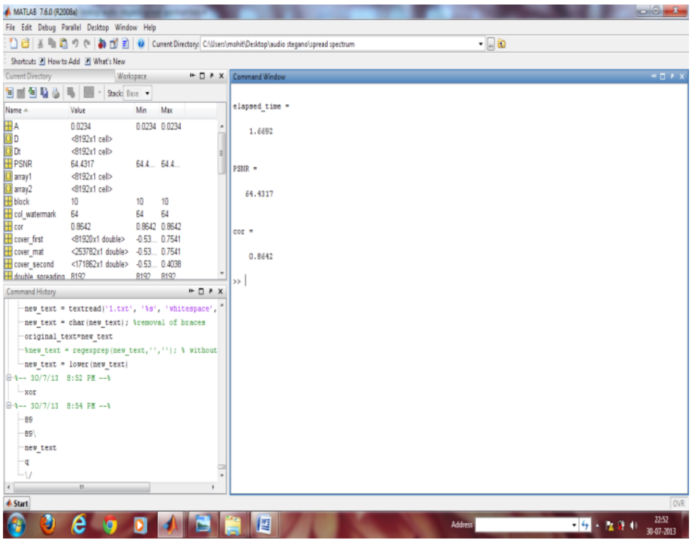


Figure 3: Comparison of Original and Extracted Watermark Image


MATLAB 7.6.0 (R2008a)
File Edit Debug Parallel Desktop Window Help
Current Directory: C:\Users\mohit\Desktop\audio stegano\spread spectrum
Shortcuts How to Add What's New
Current Directory
Workspace
Stack: Base
Command History
Command Window
Start
Address
22:52
30-07-2013

```
Name        Value             Min     Max
A           0.0234            0.0234  0.0234
D           <8192x1 cell>
Dt          <8192x1 cell>
PSNR        64.4317           64.4... 64.4...
array1      <8192x1 cell>
array2      <8192x1 cell>
block       10                10      10
col_watermark 64              64      64
cor         0.8642            0.8642  0.8642
cover_first <81920x1 double>  -0.53... 0.7541
cover_mat   <253782x1 double> -0.53... 0.7541
cover_second <171862x1 double> -0.53... 0.4038
double_spreading 8192         8192    8192
```

```
new_text = textread('1.txt', '%s', 'whitespace',
new_text = char(new_text); %removal of braces
original_text=new_text
%new_text = regexprep(new_text,'',''); % without
new_text = lower(new_text)
%-- 30/7/13  8:52 PM --%
xor
%-- 30/7/13  8:54 PM --%
89
89\
new_text
q
\/
```

```
elapsed_time =

    1.6692


PSNR =

   64.4317


cor =

    0.8642

>> |
```

Figure 4: Snapshot of Command Window for Extraction of Watermark

Table 1: Comparison of various Techniques for Psnr of Extracted Watermark

Technique	PSNR
1	31
14	42
12	45
3	46
8	49
7	51
Proposed method	64.4

CONCLUSIONS AND FUTURE SCOPE

From all the results derived from the last chapter it can be concluded that proposed methodology is much efficient in terms of PSNR, correlation with original watermark, computational time, complexity and invisibility as compared to existing other methods for the same. Proposed method is more imperceptible and a robust combined algorithm of digital watermarking, which is based on advanced spread spectrum methodology, PSNR (i.e. 103.8254 dB and 64.4317dB) and normalized correlation (i.e. 0.9995 and 0.8642) values are very high whereas, computational time (i.e. 2.2308s and 1.6692s) is very low. Performance evaluation results shows that advancement of spread spectrum methodology improved the performance of the already existed watermarking algorithms that are based solely on the normal spread spectrum methodology. The simulationresult shows that this algorithm is much better for invisible watermarking and has goodrobustness for some common signal processing operations.

This is work can be extended by improving the performance of methodology by making it more robust and less complex for low frequency audio signal. Also, time consumption for embedding as well as for extraction of watermark can be reduced.

REFERENCES

1. Youail, R.S., Samawi, V.W. and Kadhim, A-R. A- K. (2008) "Combining a Spread Spectrum Technique with Error-Correction Code to Design an Immune Stegosystem", Anti counterfeiting, Security and Identification (ASID 2008), IEEE, pp. 245-248.

2. RU, X.M., ZHANG, H.J. and HUANG, X (2005), "steganalysis of audio: attacking the steghide", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou (2005), IEEE, pp. 3937-3942.

3. Agaian, S.S.; Akopian, D.; Caglayan, O. and D'Souza S.A. (2005),*"Lossless Adaptive Digital Audio Steganography"*, (2005), IEEE, pp. 903-906.

4. Kexin, Z. (2010), "Audio Steganalysis of Spread Spectrum Hiding Based on Statistical Moment", 2nd International Conference on Signal Processing Systems (ICSPS-2010), IEEE, vol. 3, pp. 381-384.

5. Gupta, A., Barr, D.K. and Sharma, D. (2009), *"Mitigating the Degenerations in Microsoft Word Documents: An Improved Steganographic Method"*, 2nd International Conference on Computer, Control and Communication (IC4-2009), IEEE, pp.1-6.

6. Nutzinger, M., Fabian, C. and Marschalek, M. (2010), *"Secure Hybrid Spread Spectrum System for Steganography in Auditive Media",* Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2010), IEEE, pp. 78-81.

7. Gao, S.; Hu, R.M.; Zeng, W.; Ai, H.J. and Li, C.R. (2008), *"A Detection Algorithm of Audio Spread Spectrum Data Hiding"*, International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM-2008), IEEE, pp. 1-4.

8. Garay,S.H.; Medina, R.V.; Rivera, L. N. and Ponomaryov, V. (2008),*"steganographic communication channel using audio signals"*, International Conference on Mathematical Methods in Electromagnetic Theory (2008), IEEE, Odesa, Ukraine,

9. Shah, P.; Choudhari, P. and Sivaraman, S. (2008), *“Adaptive Wavelet Packet Based Audio Steganography using Data History”*, Region 10 Colloquium and the Third ICIIS, Kharagpur, (2008), IEEE.

10. Li, M., Kulhandjian, M., Pados, D.A., Batalama, S.N., Medley, M.J. and Matyjas, J.D. (2012), *“On the Extraction of Spread-Spectrum Hidden Data in Digital Media”,* Communication and Information Systems Security Symposium, IEEE (ICC- 2012), pp. 1031-1035.

11. Ghosh, S., De, D. and Kandar, D. (2012), *“A Double Layered Additive Space Sequenced Audio Steganography Technique for Mobile Network”,* International Conference on Radar, Communication and Computing (ICRCC-2012), IEEE, SKP Engineering College, Tiruvannamalai, pp. 29-33.

12. Liu, B., Xu, E., Wang, J., Wei, Z., Xu, L., Zhao, B. and Su, J (2011), *“*Thwarting Audio Steganography Attacks in Cloud Storage Systems*”*, International Conference on Cloud and Service Computing (2011), IEEE, pp. 279-284.

13. Skopin, D.E.; El-Emary, I.M.M.; Rasras R.J. and Diab R.S. (2010), *“Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal”*, International Conference on Advanced Computer Control (ICACC- 2010), IEEE, vol. 5, pp. 29-32.

14. Kumar, H. and Anuradha (2012), *“Enhanced LSB technique for Audio Steganography”,* International Conference on Computing, Communication & Networking Technology (ICCCNT-2012), IEEE-20180, Coimbatore.

15. Altun, O. ; Sharma, G. ; Celik, M. ; Sterling, M. ; Titlebaum, E. and Bocko, M. (2005) , *“morphological steganalysis of audio signals and the principle of diminishing marginal distortions”*, International conference on ICASSP (2005) ,IEEE, pp. 21-24.

16. Dastoor, S.K. (2011), “Comparative Analysis of Steganographic Algorithms intacting the information in the Speech Signal for enhancing the Message Security in next Generation Mobile devices”, World Congress on Information and Communication Technologies(2011), IEEE, pp. 279-284.